CLAIMS

We claim as our invention:

1. Apparatus comprising:

a storage device including a user area which operates in a user environment and a hidden area which stores an application requiring write protection; and

a memory coupled to said storage device and configured to be able to develop the application stored in the hidden area of the storage device, the memory providing a virtual disk space.

2. Apparatus of claim 1, wherein the storage device meets a specification selected from the group consisting of the Protected Area Run Time Interface Extension Services (PARTIES) specification and a standard specification conforming to the PARTIES specification, and wherein the hidden area is a PARTIES partition.

3. Apparatus of claim 1 wherein a boot from the hidden area in the storage device is executed with support of a basic input/output system (BIOS).

4. Apparatus comprising:

a storage device for retaining data, wherein the storage device includes:

a first partition which operates in a user environment; and

a second partition different from the first partition, the second partition storing applications requiring write protection;

wherein the second partition includes an unoccupied area in which a specific application is able to be developed when the specific application is executed from among the applications requiring write protection.

5. Apparatus of claim 4, wherein the second partition is a Protected Area Run Time Interface Extension Services (PARTIES) partition.

6. Apparatus comprising:

an external storage device which is able to form a first area operating in a user environment and a second area which is a user-hidden area; and

a basic input/output system (BIOS) which supports the booting of a predetermined application among applications stored in the second area;

a memory which is coupled to said external storage device and said BIOS and which stores code which operates on said external storage device and said BIOS when executed, wherein the stored code includes:

validation code which validates the predetermined application for a system vendor authentication; and

virtual application area forming code which copies the predetermined application onto a predetermined area selected from the group consisting of an unoccupied area in said memory and an unoccupied area within the second area, and which forms a virtual application area when the predetermined application is the validated application;

wherein an access to the predetermined application is performed in the virtual application area.

7. Apparatus of claim 6 wherein the virtual application area forming code, in forming the virtual application area, detects the size of the predetermined application and searches and secures the predetermined area.

8. Apparatus of claim 6 wherein the virtual application area forming code, in forming the virtual application area, detects the size of the predetermined

application, requests the BIOS to unlock the second area, and then forms the virtual application area in the second area.

9. Apparatus comprising:

a storage device which is divided into a user area operating in a user environment and a user-unavailable host-protected area;

a basic input/output system (BIOS) which supports a boot from the host protected area and supports a validation of an application in the host protected area which includes a system vendor authentication; and

an application access module, coupled to said storage device and said BIOS, which copies the application in the host protected area onto a predetermined area selected from the group consisting of an unoccupied area of the host-protected area and an unoccupied area of another memory, thus generating a virtual application area.

10. Apparatus of claim 9, wherein the BIOS manages a private key and an access to the host protected area.

11. Apparatus of claim 9, wherein the BIOS manages any one of a private key and an access to the host protected area.

12. Apparatus of claim 9, wherein the application access module determines whether the application in the host protected area is one that has been write-protected, and when the application is accessed, accesses the virtual application area.

13. A method comprising:

unlocking a second area when booting a predetermined application from the second area of a storage device having a first area which operates in a user environment and the second area which is an area hidden from a user;

reading the predetermined application from the unlocked second area;

locking the unlocked second area;

copying the read predetermined application onto a virtual application area formed in an unoccupied area on another memory; and

reading a first code for booting the predetermined application from the virtual application area.

14. The method of claim 13, further comprising:

determining whether the predetermined application in the second area is an application validated by a system vendor; and

detecting whether write protection is required for the predetermined application when the predetermined application is the validated application.

15. A method comprising:

unlocking a second area when booting a validated application in the second area of a storage device having a first area which operates in a user environment and the second area which is an area hidden from a user;

reading the application from the unlocked second area;

copying the read application onto a virtual application area provided in an unoccupied area in the second area; and

reading a first code for booting the application from the virtual application area.

16. The method of claim 15, wherein said reading of the first code includes reading the first code from the virtual application area by directing an access range of a disk access program toward an area onto which the application has been copied.

17. A product comprising:

a computer usable medium having computer readable program code stored therein, the computer readable program code in said product being effective to:

request unlocking of a second area of a storage device having a first area that is an operating environment for a user and the second area that is an area hidden from the user;

read, from the unlocked second area, an application which is validated by a system vendor and requires a write protection;

request locking of the unlocked second area; and

copy the read application onto a virtual application area provided in an unoccupied area on a memory different from the storage device.

18. The product claim 17, wherein the product further includes code which is effective to boot the application from the virtual application area.

19. A product comprising:

a computer usable medium having computer readable program code stored therein, the computer readable program code in said product being effective to:

request unlocking of a second area of a storage device having a first area that is an operating environment for a user and the second area that is an area hidden from the user;

read, from the unlocked second area, an application which is validated by a system vendor and requires a write protection;

copy the read application onto a virtual application area provided in an unoccupied area of the second area; and

direct an access to the application toward the virtual application area.

20. The product of claim 19, wherein the code which directs the access to the application toward the virtual application area changes an address of an access table for the application to an address of a copy destination.